CASE STUDY

SQUARESHIFT

Enhancing Network and Security Monitoring for a Leading Government Health Provider

8TB
of logs and metrics per day

14 Integrations
across Enterprise Network and security devices

10 million
events per minute

CLIENT

Our client, a pivotal government public healthcare provider, is dedicated to ensuring the seamless delivery of healthcare services across an extensive network of hospitals and Primary Health Care Clinics. With an extensive network of hospitals and Primary Health Care Clinics, the client's critical healthcare infrastructure demanded robust monitoring for seamless service delivery.

TECHNOLOGY STACK

Elastic Observability
Elastic Agent
aws
logstash
Cisco FTD Firewall
VMware vSphere
Cisco NXOS Router
Cisco Switch
Cisco Proxy

PROJECT CONTEXT

The client faced the challenge of managing a diverse infrastructure hosted on both on-premise and Cloud environments, featuring a mix of legacy and modern devices. The client wanted monitoring and AIOps capabilities, addressing the need for modern features like machine learning anomaly detection.

PROJECT OBJECTIVES

- Comprehensive Monitoring: We vigilantly oversee network components like switches, routers, and security elements, ensuring a resilient infrastructure.
- Effective Device Management: Diverse devices communicate seamlessly through SNMP and legacy protocols, enhancing network interoperability.
- Enhanced Security Measures: Implementation of Role-Based Access Control (RBAC) strengthens security by providing controlled access to both network and security teams.
- Reliable Data Flows: Proactive measures guarantee consistent data flows, even during intermittent network failures, minimizing disruptions.
- Optimized Data Processing: The project streamlines data processing, addressing challenges posed by diverse devices and ensuring compatibility

SOLUTION DELIVERY

- Developed custom adapters to seamlessly handle device data routed through syslog service and accelerators for efficient matrix processing through SNMP interfaces.
- Crafted 35 dashboards catering to both common matrices and device-specific metrics, providing a holistic view of the entire infrastructure.
- Optimized Elastic ingest pipelines to efficiently handle unsupported devices, ensuring a resilient monitoring system.
- Leveraged efficient index lifecycle policies, sharding, and Frozen tier for cost-effective data storage without compromising performance.
- Introduced logstash-based data forwarders to optimize log and metric flow, enhancing the overall responsiveness of the monitoring system.